dependent upon rejected base claims but as otherwise being allowable. Applicant respectfully disagrees with the Examiner's rejections.

Independent claims 1, 3 and 9 each provide, *inter alia*, for an access formula. Despite the fact the Carter neither teaches nor suggests anything remotely related to an access formula, the Examiner asserts that such an access formula is "inherent" in Carter.

Claim 1 provides that a value required to decrypt information is decrypted by correctly solving an access formula describing a function of groups. Each group includes a list of at least one client. A requesting consumer client is granted access to the information if the requesting consumer client is a member of at least one group which correctly solves the access formula. Carter neither teaches nor suggests Applicant's access formula.

The Examiner's support that Carter discloses Applicant's access formula is provided on page 2 as follows:

> Carter does not explicitly disclose the feature of an access formula. However, this feature is deemed to be inherent to the Carter method because the entered password would have to be compared with a stored value in order to determine granting user access (see column 16, lines 16-29; figure 4, item 90; figure 9, step 152).

There are several problems with the Examiner's argument.

First, the Examiner is abusing his discretion by not finding a teaching of Applicants' access formula.

> "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) (citations and USPQ cite omitted).
>
> M.P.E.P. § 2112.

Thus, an "access formula," by whatever definition is used, is inherent in Carter only if this is the only possible method by which a password may be verified. It is not. For example, the password may be an encoded version of the user identifier. In this case, the computer system decodes the password and compares it with the identifier. No comparison with a stored value is necessary. Since password verification methods exist which do not, as the Examiner claims,

"have to be compared with a stored value in order to determine granting user access," an "access formula," even as broadly defined by the Examiner, is not inherent.

Second, Carter does not teach a *formula* for gaining access. The passages and figures cited by the Examiner do not mention, in any manner, a formula of any kind. The text at column 16, lines 16-29, is reproduced as follows:

> After it has been determined that the document 54 to which access is requested is a work group document 90, the obtaining step 152 is performed by the collaborative access controller 44. As with other portions of the collaborative access controller 44, the portion which performs the obtaining step 152 may be embodied within the application 52 or may be a separate module which is invoked by the application 52 or by the user. The obtaining step 152 comprises interactively asking the user for its user identifier and a corresponding password. In alternative embodiments, the user identifier identifies the current user and is obtained by querying the operating system 46 or the object database system 62; only the password is obtained interactively from the user.

This passage has nothing whatsoever to do with an access formula. At best, this is a routine collection of user ID and password. The Examiner also cites Figure 4, reference 90, which is described as follows at column 12, lines 9-14:

> FIG. 4 illustrates a work group document 90, also known as "collaborative document 90," which is configured according to the present invention. The work group document 90 includes a prefix portion 92 and a data portion 94. The prefix portion 92 and the data portion 94 are each capable of being stored in at least one file in the computer system 10 (FIG. 1).

Again, not even a hint of a formula of any kind. Finally, the Examiner cites Figure 9, step 152, which bears the text "OBTAIN USER IDENTIFIER AND PASSWORD FROM USER WHO SEEKS ACCESS." Yet again, not even a hint of a formula of any kind.

The Examiner states that Carter's alleged password matching "is within the scope of an access formula as described by the applicant in the specification (see specification, page 10, lines 10-25 and figure 1, items 22 and 24)." (Page 2.) Items 22 and 24 in Figure 1 are described as follows on page 9, lines 12-18:

> Referring now to Figure 1, a diagram of a computer network that may use the present invention is shown. Computer network 20 includes a plurality of clients, shown generally by 22.

> Clients 22 may include users working on a computer which is part of computer network 20, application programs running on computers which are part of computer network 20 accessing information on behalf of a user, and automated systems which are part of computer network 20. Client systems 22 are interconnected through hubs 24 and routers 26 to form computer network 20.

How this supports the Examiner's definition of an access formula is not discernable. The passage cited by the Examiner from page 10 is as follows:

> Another design challenge is the ability to permit access to information based on combinations of groups of clients 22. A group may be defined as those clients 22 which share a common mandate. For example, possible groups may be all members of the financial department, members of the Board of Directors, software engineers assigned to project X, and the like. It is desirable to permit access to information based on combinations of groups such as, for example, clients which are either members of the Board of Directors or are members of both project X and are senior software engineers. Another useful form of description is to permit access to any client which is a member of M-of-N groups. For example, a client 22 may be granted access if it is a member of any two-of-three groups, Group 1, Group 2, and Group 3. It will be recognized that one of ordinary skill in the art can express access to information as a boolean combination of groups. A group asserts true in the boolean combination when consumer client 44 which is a member of the group requests access to the information set protected by the access formula. Consumer client 44 may then be granted access to the information if the access formula resultant is true.

As this passage indicates, access formulas may be boolean combinations of groups. Access is granted only if the logical expression is true. This is not a simple comparison of a supplied password with a stored value, as asserted by the Examiner.

Third, claim 1 provides that the access formula describe a *function of groups*. Nothing in Carter teaches or suggests such a function of groups nor has the Examiner attempted to find such a function of groups.

In addition, claim 3 provides, *inter alia*, for "acquiring a public key and a matched private key *for each of the at least one group*." It appears that the Examiner has provided no teaching or suggestion for such acquisition. In fact, Carter teaches obtaining a

public key and a private key only for each *group member*, not each group. For example, column 13, line 63-column 14, line 5, is as follows (emphasis added):

> The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the *public key of the member in question.*, which was obtained during the step 116. Note that the underlying document key is the same for each *member of the collaborative group*, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key.

Public key 78 and private key 80 are obtained for each group *member*, as is described at column 13, lines 29-46, a portion of which is reproduced as follows:

> During a member-key-obtaining step 116, the collaborative access controller 44 obtains one public key 78 for each collaborative group member. . . .
> * * * *
> In another embodiment, the collaborative access controller 44 makes requests for public keys 78 directly to the object database system 62 without going through the authenticator 64. In alternative embodiments, the public key 78 is obtained from the operating system 46, the hardware token 32 (FIG. 1), or the PCMCIA card 30 without accessing the database system 62. Similar steps are employed to obtain private keys 80 during other steps described hereafter.

Nowhere in Carter is a private key used with a group.

Claim 9 provides, *inter alia*, a group server obtaining a private key and matched public key for each group. The Examiner does not attempt to find such a teaching in Carter. As described with regards to claim 3 above, Carter does not teach or suggest obtaining such a key pair for each group.

Independent claims 1, 3 and 9 are patentable. The remaining claims depend from one of independent claims 1, 3 and 9 and are therefore also patentable. Reconsideration of this application in view of the above remarks is respectfully requested. No fees are believed to be due by filing this paper. However, any fee incurred may be drawn from Deposit Account No. 19-4545 as specified in the Application Transmittal.

The Examiner is invited to telephone the undersigned to discuss any aspect of this case.

Respectfully submitted,

JAMES P. HUGHES

By _____

Mark D. Chuey, Ph.D.
Reg. No. 42,415
Attorney/Agent for Applicant

Date: October 18, 2002

BROOKS & KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075
Phone: 248-358-4400
Fax: 248-358-3351